

DETAILED ACTION

1. This correspondence is in response to **AMENDMENTS and REMARKS** filed on 09/22/2009.
2. **Claims 19, 21, 23-36 and 39** are pending. Claims 1-18, 20, 22, 37-38 and 40 are canceled.

Response to Arguments

3. Applicant's arguments with respect to the rejection of the pending claims over prior arts of record have been fully considered and are persuasive. The rejections of Claims 19, 21, 23-36 and 39 have been withdrawn.

Allowable Subject Matter

4. **Claims 19, 21, 23-36 and 39** are allowed. No reason for allowance is needed as the record is clear in light of further search conducted and applicant's arguments filed on 08/31/2009.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Eric G King on 10/20/2009

6. The application has been amended as follows:

In the claims,

Claim 33(Currently Amended) A method for secure communication of message (m) sent by any one individual member (M) of a group (G) using a group signature (S), storing, using a group signature device, personalized data (z, Kz) that identifies said one individual member (M) of the group (G); storing, using the group signature device, a predefined private signature key(SK) that is common to all members of the group(G); producing, by said one individual group member (M), the group signature(S) of the message (m) on behalf of the group(G) by signing, with said predefined private signature key (SK) common to all group members stored on said group signature device, a set including the message(m) and a single encrypted text(C) produced using a personalized data (z, Kz) of said one individual member (M) only; and outputting the message (m) along with the group signature (S) to a checker, such that the checker, upon receiving the message accompanied by the group signature, is able to verify that the message (m) is associated with the group (G) based on the group signature (S), with the identity of the individual member (M) of the group (G) remaining anonymous to the checker.

Contact Information

7. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays should be clearly labeled "Comments on statement of Reasons for allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 5712738300. The fax phone number for the organization where this application or proceeding is assigned is 571-272-4195.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Fikremariam Yalew/
Examiner, Art Unit 2436
10/20/2009

/Nasser G Moazzami/
Supervisory Patent Examiner, Art
Unit 2436